



Vaasan yliopisto
UNIVERSITY OF VAASA

OSUVA Open
Science

This is a self-archived – parallel published version of this article in the publication archive of the University of Vaasa. It might differ from the original.

Ethics of Security: From Personal Safety to Cyber Security

Author(s): Lehtonen, Tommi

Title: Ethics of Security: From Personal Safety to Cyber Security

Year: 2021

Version: Publisher's PDF

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited

Please cite the original version:

Lehtonen, T. (2021). Ethics of Security: From Personal Safety to Cyber Security. In: Taskiran, M. N. & Pinarbaşı, F. (eds.) *Multidisciplinary Approaches to Ethics in the Digital Era*, 44-59. Hershey, PA: IGI Global.
<https://doi.org/10.4018/978-1-7998-4117-3.ch004>

Chapter 4

Ethics of Security: From Personal Safety to Cyber Security

Tommi Lehtonen

 <https://orcid.org/0000-0002-0286-3059>

University of Vaasa, Finland

ABSTRACT

This chapter aims to identify and analyse the ethical problems of security, particularly cyber and digital threats. The concepts of security and safety are defined based on existing literature. The chapter addresses the key results and research gaps in the field (i.e., security issues in different areas) and future challenges, both theoretical and empirical. Moreover, the discussion is linked to an analysis of the relationship between utilitarian ethics and deontological ethics, which brings a new perspective to the debate on security ethics in general and cybersecurity. Finally, comprehensive security and absolute safety ideas are discussed, which sheds new light on the complexity of security concerns.

INTRODUCTION

This chapter identifies and analyses the ethical problems of security, with special reference to cyber and digital threats. Amid the growing global threats of climate change and economic inequality, one might find it tempting to define ethics as prescriptions to prevent humans from hurting each other and the rest of the biosphere. From this it can be deduced that ethics is essentially about security, in various forms, and that other important aspects of ethics such as fulfilling one's duties, developing virtues and character strengths, feeling empathy and reinforcing pro-social behaviours ultimately serve the same goal: security, both personal and collective. This view means that the ethics of security is not merely a subfield or special area of ethics, but the core and epicentre of ethics. However, it is possible to remark that emphasising security easily leads to employing ethics as a means to an end, which anchors ethics firmly in one particular paradigm and tradition, namely utilitarianism or consequentialism. To this, the reply can be that nothing automatically forces one to formulate and establish ethics in general, or the ethics of security in particular, merely based on utilitarian premises, but also other theories such as deontological ethics, contractarianism, virtue ethics and care ethics play an important role in the ethics

DOI: 10.4018/978-1-7998-4117-3.ch004

of security (see Table 1). The contribution of different ethical theories to security considerations will be discussed in this chapter.

BACKGROUND

The United Nations Development Programme (UNDP) included the phrase *human security* in its 1994 report, which triggered a debate about the perception of security. That debate has challenged an earlier understanding of security that emphasised the sovereignty of national states, the importance of defence politics and international negotiations and treaties (Martin & Owen, 2015, 1). The present understanding of human security hovers around human development and human rights and even national security, but it is wider than any of them alone (Sen, 2015, 18). In addition to these wide-ranging issues, Amartya Sen points out a much more narrow and personal interest in security: the majority of people are concerned with the security of their own lives and of the lives of their family members (ibid.). Sen emphasises that this general concern has to be addressed and any understanding of security can be integrated with it to the extent that this makes human life more secure. Such an integrative understanding of human security is important precisely because it affects human lives. National security and global security alone, without the integration with an individual's "world of experience", are more abstract entities and, often, more remote from everyday life. These political forms of security are frequently defined in terms of military or ecological preparedness and other modes of national and international problem-solving.

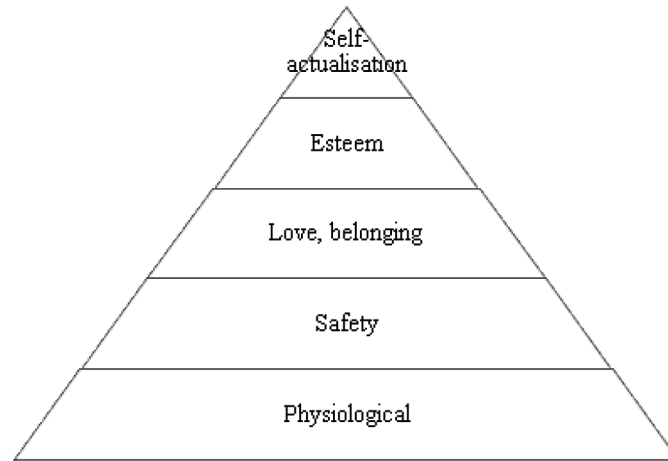
With security being a matter of personal interest, it is worthy to pay attention to the underlying psychological background. Scholars in various fields have argued that security is a basic human need (Maslow, 1943, p. 376–380; Staub, 2003, p. 2; Doyal & Gough, 1991, p. 214–213). Famously, Maslow ranked security or safety as a psychological need second to the basic physiological needs such as air, water and food. Maslow's hierarchy of needs is often represented as a pyramid in which the bottom represents basic biological drives for survival (Figure 1). Other basic needs, such as the need for safety, love, esteem and self-actualisation, are also universal, but not absolutely necessary for survival. Moreover, a desire to sacrifice oneself for others does not necessarily go against the need for survival or safety, because self-sacrifice can serve the greater good of the survival and safety of a collective, such as a family, clan, race or nation. However, the higher one climbs in the hierarchy of needs, as more specific desires are addressed along the way, the more suspicious one may become of the universality of human needs. Maslow (1943, p. 389) said, "Certainly in any particular culture an individual's conscious motivational content will usually be extremely different from the conscious motivational content of an individual in another society. However, it is the common experience of anthropologists that people, even in different societies, are much more alike than we would think from our first contact with them, and that as we know them better we seem to find more and more of this commonness".

DEFINITIONS

With these background remarks in mind, the concepts of *security* and *safety* need to be defined and analysed. No concept exists in isolation from other concepts and linguistic practices (Gasper, 2015, 33). Therefore, to understand *security* and *safety*, it is necessary to be familiarised with the real-world contexts of users and audiences of those words, purposes within those contexts and accumulated patterns of use

Figure 1. Pyramid showing Maslow's hierarchy of needs

Source: (the author, 2019)



of the words concerned. In what follows, defining *security* and *safety* takes place primarily based on the United Nations characterisations and relevant research literature. Worth special mention is the *Routledge Handbook of Human Security* (2015). The definitional task under discussion is all the more important because the concepts of *security* and *safety* are ambiguous and complex, as will be seen hereafter.

Let us start with some everyday observations about the uses of the terms *safety* and *security*. It is easy to identify examples of expressions where safety means a tool or measure that reduces hazards. Safety can also mean a place or position where there is no danger (Martin & Owen 2015). Thus, in security considerations, the benefit pursued is understood in terms of the pair of safety and danger. For example, family, friends and paid work can be part of one's safety net. For many, a home is a shelter and safe haven.

Security, for its part, is a state where threats and risks can be controlled. Even if such a state can be assessed objectively, security is also a matter of subjective experience. Therefore, one person may feel safe in a situation where another person feels insecure. The objective and subjective aspects of security do not always go hand in hand.

Moreover, security is relative in two ways. First, security is always relative to a real or imagined threat. Viruses, worms and attacks from hackers can potentially threaten any computer connected to the internet. The computer system can be safeguarded from cybersecurity threats with a firewall and virus protection software. Secondly, there are degrees of security. Someone or something can be safe from a risk or danger, i.e., they cannot be affected by it. However, something else can be an even safer option, and the safest option is in many cases the most recommendable to choose, unless one is ready to accept risks such as those related to share trading.

Let us continue our definitional task by leaning on the United Nations 1994 *Human Development Report* and the 2003 report of *Human Security*. In light of them, security can be defined as the condition of being protected from harm or other unwanted outcomes caused by intentional human action. Safety, in turn, is the condition of being protected from harm and injuries, caused by unintentional hazards. Thus, the concepts of security and safety are interrelated but distinguishable based on their being caused by human or natural factors – a topic discussed by philosophers specifically in the context of the problem of evil. Human or moral evil refers to harm and suffering caused by intentional human actions or

behaviour, subject to moral evaluation. Natural evil refers to natural disasters and other harm and evil caused by natural phenomena such as disease and dysfunction. However, the distinction between moral and natural evil is not razor-sharp or unambiguous. The necessary preconditions for many accidents include human practices (e.g. transportation, energy production and consumption, residential activities and industrial processes) and technology created by humans even if the accidents themselves are non-intentional, and in that respect, represent natural evil rather than moral evil (Neiman, 2015, 23). In its widest sense, the phrase *human security* refers to the condition of being protected both from intentional and non-intentional harm and from both moral and natural evils.

Des Gasper identifies different definitions of security according to their range. In the widest range, human security includes the promotion and expansion of capabilities that strengthen existing opportunities and create new possibilities for human flourishing (Gasper, 2015, 33). These capabilities include all skills and faculties considered as good and useful and which humans, both as individuals and as members of social and cultural groups, can have innately or can learn to do. Taking this into account, security can be defined as a condition under which human flourishing is maximally possible and maximally sustainable.

SECURITY AS SUSTAINABILITY

The widely accepted definition of sustainable development is that used in the Brundtland Report: “Sustainable development is development that aims to meet the needs of the present without compromising the ability of future generations to meet their own needs” (The World Commission on Environment and Development, 1987, 8). Although this is a vague statement, it has proved durable.

The term *sustainability* is often preferred over *sustainable development*. Development may be perceived as implying growth and, therefore, sustainable development means mitigating the problems caused by, but not necessarily challenging, continued economic growth (Lehtonen, 2016, 191, 193).

The concept of *sustainability* can be used in different ways in relation to security or safety. Environmentalists mean ecological well-being and security when they speak of sustainability. Many business-people really mean economic performance and security reflecting the efficiency of businesses when they speak of sustainability. From a more general perspective, sustainability is said to have three major aspects – ecological, social and economic – and it is not possible to achieve a particular level of any of them independently without achieving at least a basic level of all three forms simultaneously (Frigo 2018, 84). This shows that security, as a sum of sustainability, is a complex concept and phenomenon. Thus, it is not possible for subsystems to be secure and sustainable within an unsustainable global system. Security and sustainability are properties of the Earth system as a whole, including the interacting physical, chemical and biological processes and global social, political and economic developments. Therefore, a business or organisation is unlikely to be sustainable if the society at large is not secure.

PEOPLE-CENTRED SECURITY

In the current understanding of security, the 1994 *Human Development Report* and the 2003 UN report of *Human Security* are the major sources. The *Human Development Report* points out that for many people today, a feeling of insecurity arises more from worries about everyday life than from the fear of a global catastrophe, even if many people are concerned about climate change. Job, income, health, one’s own

children – these are the major human concerns all over the world. Therefore, the report defines security as “safety from the constant threats of hunger, disease, crime and repression”. Thus, the report sees security, both individual and social, as the condition of being protected from both moral and natural evils. Moreover, the report characterises security as “protection from sudden and hurtful disruptions in the pattern of our daily lives – whether in our homes, in our jobs, in our communities or in our environment” (UNDP, 1994, 3). Thus, the report takes into account both individual and social dimensions of security.

In the same report, human security is considered a global concern and relevant to people both in rich countries and poor. Unemployment, alcohol and drug abuse, crime, pollution and violations of human rights pose real threats to many people. These threats are persistent and continuously evolving, even though their intensity differs from one place to another. In addition, different security concerns are interdependent. When the security of people is jeopardised anywhere, other nations may get involved through various relationships and dependencies. Famines, pandemics, pollution, drug trafficking, terrorism, ethnic disputes and social disintegration are not confined within national borders. Their consequences can affect all people. Therefore, human security is easier to ensure through early prevention than later intervention (UNDP, 1994, 22-23).

According to the *Human Development Report*, threats can be accumulated and can lead to persisting disparity between ethnic groups or between regions. Violence can follow from social inequalities in power and economic opportunities. When people see their security threatened, they often become less tolerant, as the rise of nationalism and right-wing populism worldwide shows (UNDP, 1994, 23).

The 2003 UN report links human security to the protection of fundamental freedoms. In this vein, the report outlines security as the protection of people from critical and pervasive threats. That protection is achieved by collaboration between social systems representing different interests and values such as environmental, economic and cultural. The social systems concerned include democratic decision-making, the armed forces and environmental protection organisations, among others, and together they establish the requirements for a dignified life and human survival (United Nations Commission on Human Security, 2003, 4).

Both UN documents considered here argue for the concept of security that is people-centred. The reports see that security consists of different interrelated dimensions such as environmental, economic and military. The lack in one dimension does not usually propel a displacement into another. Rather, the lack of security in one dimension is apt to add to insecurity in another dimension. For example, environmental threats can lead to economic threats, which can undermine mood and expectations in a society and can result in depression and poverty. These interlinked factors create a web of risks that threatens human security. Therefore, to analyse the relational ontology and moral psychology of threats is necessary for understanding the requirements for security. With this in mind, a short overview of security concepts is provided from the perspective of different ethical theories.

SECURITY FROM THE PERSPECTIVE OF DIFFERENT ETHICAL THEORIES

According to utilitarianism (or consequentialism), the ethics of security aims at benefits (e.g. peace, well-being and prosperity) and safety necessary for both individuals and societies. In the ethics of duty or deontological framework, the ethics of security focuses on duties, related to the protection of basic and human rights, the following of which is a universal responsibility and which the human reason can recognise as a universal obligation. The Universal Declaration of Human Rights (UDHR) and the United

Ethics of Security

Nations reports on human security remain in this deontological framework. In contractarianism or a social contract framework, the ethics of security focuses on treaties and conventions made for enhancing security and stability in a society and between countries. Virtue ethics tries to determine and explain the character and communal traits that are necessary for security and that can be created by upbringing and education. Ethics of care, for its part, sees security both as the fruit and foundation of caring relationships and practices.

Table 1. The approach to security in different ethical traditions

	Idea of Security	Why Is Security Important?
<i>Utilitarianism</i>	Security is the goal of ethics and the ultimate benefit of doing good deeds.	Security is required to achieve a variety of other good things (e.g. peace, well-being and prosperity) important for a society.
<i>Ethics of duty</i>	The ultimate ethical duty is to contribute to the security of individuals and communities.	To actively contribute to the security of other persons means treating them as an end in themselves.
<i>Social contract theory</i>	Security is based on legislation, treaties and conventions.	Security is one of the benefits all members of a society can benefit from and one of the hallmarks of a good society.
<i>Virtue ethics</i>	Security requires peaceful and just societies with individuals who have virtues such as practical wisdom, courage, modesty and fairness.	Living in a safe society under good governance enhances the possibility of developing virtues and character strengths.
<i>Ethics of care</i>	Caring brings about security that is the basis for the healthy development of children and adolescents.	Security is both the fruit and foundation of care.

Source: (the author, 2019)

The foremost task of deontological ethics is to demarcate the area of permitted conduct and actions from the area of prohibited conduct and actions. In the field of cyber and digital security, this means building and programming security systems in which the algorithms contain demarcation rules to distinguish between permitted and forbidden “moves”. These demarcation rules are comparable to the constitutive rules that define different games (Myerson 1997). In order to realise the demarcation requirement, an algorithm may need to refer to a list of forbidden activities. An advanced deontological system can also learn new rules and situational exceptions based on relevant documents such as legal texts, policy papers and scientific studies (Togelius 2011).

The role of utilitarian ethics in a computerized security system, for its part, is to optimise the decision-making and operations in the area of safe activities and unsafe activities. In this view, utilitarian ethics can be compared to strategic rules that define how the game is played optimally and with a winning strategy. This requires the creation of algorithms that can compute feasible and optimal courses of action in different situations (Boddington 2017; Bonnefon et al. 2015, 2016; Brant 2016). The classic utilitarian maxim paves the way for such an algorithm: “Get the best possible benefit for the largest number of people”.

APPROVING RECOGNITION AS A KEY PREMISE OF SECURITY

According to Hegel, human life in society is the struggle for recognition. Although this characterisation has most often been understood to refer to the value and identity of individuals, the concept of recognition is also relevant when considering the safety and security of groups and communities such as ethnic groups and cultural minorities. By recognition, Hegel means identifying a person as having certain rights and responsibilities. By means of the United Nations Universal Declaration of Human Rights (UDHR) (1948), the member countries recognise human individuals and collectives (e.g. people, nations; ethnic, religious and cultural groups; minorities) as having certain rights and responsibilities. Article 3 of the Universal Declaration of Human Rights guarantees security of the person, and the European Convention on Human Rights also mentions and protects that right.

If an individual or a collective has been granted certain rights, such as security and freedom of expression, that is usually taken to imply that the individual or collective in question should assume the related duty to respect the rights of others. Thus, there is a universal duty to respect the security of other persons. However, this is not automatically the case as individuals and groups can easily overlook the fact that everyone else has the same basic rights. This is one reason why the requirements and conditions for recognition are a relevant topic for both individuals and societies.

Axel Honneth points out that the denial of recognition creates social struggles and undermines security. Specifically, the emotional experiences related to attitudes and actions of others towards oneself make one feel that he or she is being recognised or being denied recognition. If recognition is denied, one may feel insecure. Negative emotions can reveal to one that an injustice is taking place or that one is not being adequately recognised. However, negative emotions do not automatically reveal that one is disrespected or unsafe (Honneth, 1995, 138). What they provide is the possibility to identify an injustice or insecurity to be opposed. In this way, the experience of insecurity is a psychological force behind social struggles. Further, experiences of insecurity can provide the basis for political struggles in circumstances conducive for a social movement (Honneth, 2007). Insecurity can also result in retreat, or random resistance. The recognition of universal human rights, security included, attempts to prevent these maladies. This analysis locates the source and justification of social struggles in the lack of recognition (Fraser & Honneth, 2003, 174; Honneth, 1995, 168). Thus, for social and political security, recognition is a necessary condition.

CYBER SECURITY AND NEIGHBOURING CONCEPTS

It has already become clear that security is a complex concept and phenomenon. This complexity also concerns cyber security. In what follows, new light is shed on the major challenges of cyber security by identifying and defining key concepts that hover around the security risks related to digital technology.

The world relies on digital technology and algorithms more than ever before. As a result, digital data creation, use and storing soar. Today, individuals and collectives, including industries and governments, store data on computers and transmit it across networks to other computers. This global data system has vulnerabilities that can undermine the rights and well-being of individuals and damage the objectives of organisations (Eggenschwiler, 2017; Fichtner, 2018).

Moreover, secret and anonymous algorithms threaten privacy and even the rule of law. Imposing fines or taxes, judging somebody guilty or sending people to jail because of the inexplicable, unchallengeable

judgments of computer programmes undermines legal systems. Such programmes and algorithms are “black boxes”, i.e., systems, whose inputs and outputs are known, but whose internal working is not well, or at all, understood. In view of this, cyber security is not merely a technological challenge but is very much a matter of using information ethically and making morally right decisions based on information.

Cyber security protects computer systems from unauthorised access or being otherwise damaged. Thus, cyber security is, primarily, the practice of defending data systems from malicious attacks (Pernice 2019).

Cyber security can also be characterised as an endeavour that strives for security in an electronic and networked society. Accordingly, cyber security recognises, prevents and prepares for the impact of disruptions in electronic and networked systems. Thus, cyber security aims to ensure the integrity, privacy and availability of information. Such security is comprised of tools, technologies and best practices designed to protect data systems from attacks.

Cyber security is also known as information technology security and electronic information security. Because of these neighbouring terms, cyber security is apt to be confused with information security. Information security is a broader category and aims to protect all information assets, whether in physical or digital form. It focuses on securing the availability, integrity and confidentiality of data. In this way, information security is a key element in the quest for cyber security.

In recent years, cyber security gained wide media attention (for example relating to election campaigns, data privacy compromises and sexual misconduct cases) and the lack of security has created an increasing pressure of litigation. These developments can be attributed to a substantial increase in cyber attacks and their significant impact on individuals and organisations. Cyber attack is a broader concept than data network attack because it can also be done in ways other than through a data network. In view of this, the relationship between cyber attack and data network attack is similar to that between information security and cyber security: the first mentioned is a major concept, and the second one a sub-concept.

As seen, cyber security is a concern of a digital and networked society and organisation. The operational environment of digital systems can be trusted and protected in the state of cyber security. At the same time, the purpose is to secure the functioning of a digital and networked society or organisation. Cyber security includes measures that can be used to manage in advance and, if necessary, tolerate various cyber threats and their effects. Cyber threats are potentially harmful events affecting information systems.

Digital security makes use of the tools to shield one’s identity, assets and technology in the online and mobile environments. Thus, digital security refers to various ways of protecting one’s internet privacy and email and other digital accounts from intrusion by outside users. The tools one can use to protect his or her identity include antivirus software and web services, biometrics and secure personal devices such as smart cards, smartphones and e-passports. People carry these devices with them daily. The mere fact that these devices are used on a daily basis makes them vulnerable to various kinds of attacks, as people easily forget the risks related to daily activities. In an age of nonstop hacks and data breaches, getting a handle on one’s own digital security matters more than ever. Moreover, every organisation has to take care of digital security.

A data breach can have devastating consequences for any business. It can destroy a company’s reputation and can cause the loss of consumer and partner trust. The loss of critical data can cost a company its competitive advantage. A data breach can also impact corporate revenues due to violation of data protection regulation. It is estimated that, on average, a data breach costs an affected organisation more than four million dollars. Therefore, it is essential that organisations and societies adopt and implement a strong cyber security policy (Eggenschwiler, 2017; Dutton, 2017).

TYPES OF CYBER THREATS

Common cyber threats include computer viruses, spyware, ransomware, and phishing attacks. Traditional cyber security focuses on the implementation of defensive measures (e.g. strong antivirus software and good security habits such as using strong passwords and not using the same passwords) around a defined environment such as an organisation's intranet or home. Recent developments like increasing remote work and portable devices have dissolved the digital environment, reduced physical presence and visibility into cyber activity and expanded the attack surface (Eggenschwiler, 2017; Fichtner, 2018; Pernice 2019).

Today, digital breaches are rapidly increasing despite record levels of security spending. Global organisations are moving to a human-centric approach that places focus on changes in user behaviour and the essential skills of a digital citizen instead of digital countermeasures. Based on behaviour analytics, human-centric cyber security focuses on how an end-user interacts with data and applies security controls in various data systems. Ultimately, this approach is designed to identify behavioural threats in order to reveal the most serious risks, reducing investigation and threat detection time.

Many critical functions in society, such as money, energy, water and air traffic control, are dependent on the operation of information systems and networks. Faults in systems and networks that support these functions may be caused by security issues such as malware or malfunctioning devices.

THE RELATIONSHIP BETWEEN SECURITY AND SUSTAINABLE DEVELOPMENT

The concept of sustainability was briefly mentioned above. In what follows, a closer look at the relationship between security and sustainable development is taken. The concern over climate change and the depletion of natural resources, among other things, has prompted many citizens to re-evaluate the scope and limits of economic growth and examine more closely the notion of sustainable development. That is largely a security issue in terms of both personal and social concerns. The promotion of social justice and safeguarding of human rights have also been portrayed as demands directed towards societies and businesses (Smith et al. 2010). Such demands are understandable because in the global economy, large companies and corporations have significant political power and resources. Thus, business life plays a large role in both economic security and social equality, both of which are important aspects of sustainable development and of a just society. Therefore, safety at work and secure employment are important aspects of security in people's everyday life. Further, people throughout the world are united in their concern over environmental, social and corporate governance issues, i.e., issues of social responsibility. These issues are closely related to security concerns that arise from climate change and other ecological threats and from increasing social inequality and the widening of income gaps. Since the concept of sustainable development is often mentioned as a remedy or cure for these calamities, there is every reason to pay attention to sustainable development as a relevant aspect of security.

The concept of sustainable development is vague and often coloured by unexplicated economic, political, and ideological background assumptions. Such background assumptions include the ideology of continuous development, the pursuit of profit maximization, the intrinsic value of life and nature, and, among others, the animal liberation thought. The clarification of background assumptions is important because they function as the presuppositions and motives of sustainable development and determine the objectives of security considerations in a global setting. Then again, the recommendations for ac-

tion related to sustainable development can be similar irrespective of background assumptions. Thus, the background ideologies of sustainable development are not necessarily mutually exclusive but can be concurrent.

Sustainable development, in the widest sense of the word, is said of any positive change. Therefore, sustainable development looks like a cloud and its edges are hazy. It is not, however, a dry cloud but electrically charged: different aspects of sustainable development resist each other. Consequently, the concept of sustainable development has been criticised for the reason that poorly compatible ingredients such as economic growth and environmental protection are counted to belong to sustainable development. These tensions make sustainable development a complex, if not problematic, premise and approach for security considerations. Generally speaking, security always consists of a variety of aspects and ingredients, which means that achieving good comprehensive security may require compromises in many details and sub-aspects of security.

As mentioned, the most often referred definition of sustainable development is that of the 1987 Brundtland Report. According to it, sustainable development meets the needs of the present without compromising the ability of future generations to meet their own needs. This definition suggests that there should be a joint effort of the present generation to give the next and subsequent generations a healthy and secure society in all respects. Anthropologist and historian Joseph Tainter (2006, 92) criticises this definition as being too wide and general.

According to Tainter (2006, 92-93), sustainability is a matter of solving complex ecological, economic and social problems. Thus, sustainability is based on the ability to solve problems. One might want to add that major problems include global security issues.

Tainter says that sustainability in the long term requires understanding and controlling complex problems. His central, but not completely uncontroversial, claim is related to this: Complexity grows when social problems are attempted to be solved at the same time when costs are going up. Complex social solutions can both support and prevent sustainable development and security. Therefore, Tainter separates (2006, 94) three different results that can arise from attempts to solve big problems: social collapse, simplification, and increasing complexity. Especially the first and the last ones increase insecurity.

The control of growing complexity continuously requires more investment and energy. As the costs of problem-solving grow, the point will finally be reached where no additional investment generates a corresponding gain, but risks and insecurity gain ground (Tainter, 2006, 94). The complexity that is created by solving problems can enhance society's sustainability, but also lead to insecurity and destruction (Tainter, 2006, 100).

Thus, Tainter criticises the definition given by Brundtland and claims that sustainability is an active condition for solving problems – not a passive consequence of reducing consumption, as Brundtland suggests. Therefore, sustainability requires more resources, not the reduction of consumption. Therefore, we must afford sustainability in the same way as we must afford security. On the other hand, the costs of sustainability can endanger and destroy the whole society (Tainter, 2006, 99).

Tainter's view can be illustrated by comparing the whole of ecological, economic and social sustainability to a complex machine. Resources and sophisticated measures are required to haul and renew the machine part by part so that it does not shut down, but keeps moving, safely, all the time.

I have already mentioned climate change as a major threat to sustainable development and global security. The key facts about climate change are well known. Peter Singer (2016, 130-131) summarises them as follows: "Our planet's atmosphere has already absorbed such a large quantity of human-produced greenhouse gases that global warming is underway, with more extreme heat waves, droughts and floods

than ever before. Arctic sea ice is melting, and rising sea levels are threatening to inundate low-lying densely populated coastal regions in several countries. If rainfall patterns change, hundreds of millions of people could become climate refugees.”

Singer (2016, 131) also points out that an overwhelming majority of scientists in the relevant fields believe the following: the Earth is “on track to exceed the level of global warming at which feedback mechanisms will kick in and climate change will become uncontrollable, with unpredictable and possibly catastrophic consequences.”

Moreover, it is often pointed out that the affluent countries have caused the problem, “owing to their higher greenhouse gas emissions over the past two centuries. They continue to have the highest levels of per capita emissions, and they can reduce emissions with the least hardship. There is no doubt that, ethically, the world’s developed countries should be taking the lead in reducing emissions” and thereby contributing to global security. (Singer, 2016, 131.)

Singer (2016, 131) also calls attention to the fact that continuing global population growth undermines “the impact of whatever emission reductions affluent countries can be persuaded to make”. Thus, besides the use of fossil fuels, global population growth is another major driver of climate change and another major threat to global security.

Singer (2016, 131) refers to four factors that influence the level of emissions: economic output per capita, the units of energy used to generate each unit of economic output, greenhouse gases emitted per unit of energy, and total population. “A reduction in any three of these factors will be offset by an increase in the fourth. [...] globally, economic and population growth continue to be the ‘most important drivers’ of the increase in CO₂ emissions from fossil-fuel combustion.” (Singer, 2016, 130-131.) Thus, also in the context of climate change, security consists of a variety of aspects, which implies that security requires bargaining and compromises.

COMPREHENSIVE SECURITY

I have mentioned the concept of comprehensive security. Comprehensive security can be defined as a state of preparedness for threats and risks to vital functions of society. Thus, the term *comprehensive security* refers to the fact that security consists of a variety of components. It consists of components because there are many threats and dangers. In what follows, some major components are identified and analysed.

An individuals’ sense or feeling of security is made up of a variety of matters, some of which are more important than others. For example, getting a job or recovering from a serious illness can significantly increase a person’s sense of security. However, the sense of security associated with individual things easily fades over time. One begins to take health and workplace for granted, and they may no longer increase the sense of security, especially if new concerns have appeared on the horizon.

The comprehensive security of a society means an objective state where the whole is more than the sum of its parts. It is about coordinating and developing the various aspects of security, such as cyber, energy and environmental security. It requires decisions and measures that cross the boundaries of administrative sectors and businesses. It also requires organisations and special officials with the task of planning and steering the coordination of various components.

Comprehensive security has its internal and external aspects and has a political dimension and a geographical dimension. Internal security includes social balance, economic and political stability, clean nature, the ability to deal with the refugee crisis, with the threat of terrorism and other security threats,

and in principle all that strengthens democracy and the well-being of citizens. Thus, schools and social and health services also represent internal security.

External comprehensive security includes the fight against military threats, peace in the near abroad and the world, the ability to combat climate change and other cross-border environmental threats, the resolution of refugee problems, the prevention of trade wars and international terrorism, and so on. External comprehensive security has traditionally been treated as a security policy issue. The cornerstones of security policy are foreign and defence policy, but comprehensive security also has dimensions of commercial and environmental policy.

Comprehensive security is taken care of so society can maintain its ability to function even in difficult circumstances and to recover quickly from disruptions. Comprehensive security is also provided so individuals and groups can live in peace and feel safe.

One can feel safe if one does not understand what it is to fear. However, one can also feel safe when he or she realises that caution is needed. Such security is related to self-knowledge and confidence.

Security is also a social construct the need for which is created by identifying threats and painting doomsday scenarios. The sale of insurance, alarm systems and survival kits are based on this. It is also the basis of the arms trade.

The authority responsible for comprehensive security is “in danger of shooting himself in the foot” by emphasising threats and security solutions. Knowledge increases pain, and risk awareness increases insecurity. Therefore, the cheapest way to increase overall security is to avoid public discussion of the topic.

This, of course, requires that security is not already shaken and fear has not conquered the mind. Secrecy would then only aggravate the situation. When fear is on, the most affordable way to increase comprehensive security is through calm speech and behaviour. In addition, other security solutions can be available. They come in many qualities and prices. Not all threats have a solution, but it is not always known in advance what threats cannot be solved.

Citizens prefer to hear bad and insecure news rather than “radio silence” from the authorities. Recently, bad news has been heard on climate change, the world economy and international politics. Security is shaken. Still, many people would rather be aware of the situation than to be ignorant. They consider truth and honesty more important than a sense of security.

ABSOLUTE SAFETY

Have you felt safe and secure so that no matter what happens, nothing can hurt you?

According to national and international surveys, security is a major value for both individuals and communities (Pew Research Center, 2019). However, security is relative in two ways. First security is related to a real or perceived threat, and second, there are degrees of security: safe, safer, safest.

Ludwig Wittgenstein talked about the experience of feeling absolutely safe: “I mean the state of mind in which one is inclined to say ‘I am safe, nothing can injure me whatever happens.’” (Wittgenstein, 1965, p. 8). Such a feeling is not coming from the home alarm system or the Government Security Committee.

Absolute safety can be felt for a variety of reasons and in different life situations. The feeling may be related, for example, to the experience that one’s life is related to a larger whole or to a story larger than oneself. The feeling of absolute security is strengthened if one can think that not all dignity will be lost to death.

People have a lot in common and have more in common than any individual. While each one of us dies, the good in person, who is not ultimately private but common, continues in new individuals. This good, which reincarnates and receives new manifestations, is the cognitive and artistic heritage of humanity. Values and virtues also reincarnate and rise like a phoenix from the ashes. They are worth preserving and essential to the future of humanity. Therefore, it is necessary to direct our energies towards the virtues and to focus on their promotion, in the end for fair humanity.

However, humanity is not eternal. The sun also dies out someday. Therefore, does mortality pull the absolute sense of security under the rug? Wittgenstein drew attention to this and wrote: "To be safe essentially means that it is physically impossible that certain things should happen to me and therefore it's nonsense to say that I'm safe *whatever* happens." (Wittgenstein, 1965, p. 9.) Yet, one of the most prominent philosophers of the last century said he felt absolute security.

So how is it? Does humankind's mortality make the sense of absolute security meaningless? At least it can be said that it requires idealism to think like this. Whatever happens to humanity, it is better that humans have had virtues such as wisdom, self-control, courage and justice. Having these and other virtues is permanently better than never having them. Whatever happens, nothing threatens human totally, for the highest in humans are those enduring values, no matter how imperfectly they are realised in us.

Despite its universe-embracing nature, the experience of knowing absolute security is personal. Only an individual can feel safety or anything in the first place.

SOLUTIONS AND RECOMMENDATIONS

Security is a basic human need and thus an essential part of wellbeing. The majority of people are concerned with the security of their own lives and of the lives of their family members. Any understanding of security must be integrated with this general concern. Moreover, a number of international treaties define security as a basic human right.

Secret and anonymous algorithms threaten privacy and the rule of law. Imposing fines or taxes, judging somebody guilty or sending people to jail because of the inexplicable, unchallengeable judgments of computer programmes undermines legal systems. In view of this, cyber security is not merely a technological challenge but very much a matter of using information ethically and making morally right decisions based on information.

Human-centric cyber security focuses on how an end-user interacts with data and extends security controls into all data systems. This approach identifies behavioural threats in order to reveal the most serious threats, reducing investigation and threat detection times.

FUTURE RESEARCH DIRECTIONS

Big security concerns arise from climate change and other ecological threats and from increasing social inequality and the widening of income gaps. Since the concept of sustainable development is often mentioned as a remedy or cure for these calamities, there is every reason to pay attention to sustainable development as a relevant aspect of security.

CONCLUSION

Security is relative in two ways: security is always relative to a real or imagined threat, and there are degrees of security. In the widest range, human security includes the promotion and expansion of capabilities that strengthen existing opportunities and create new possibilities for human flourishing.

In a utilitarian framework, the ethics of security aims at peace, well-being and prosperity, necessary for both individuals and societies. In a deontological framework, the ethics of security focuses on duties related to the protection of basic and human rights, the following of which is a universal responsibility and which the human reason can recognise as a universal obligation. In a social contract framework, the ethics of security focuses on treaties and conventions made for enhancing security and stability in a society and between countries. Virtue ethics tries to determine and explain the character and communal traits that are necessary for security and can be created by upbringing and education. Ethics of care sees security both as the fruit and foundation of caring relationships and practices. In view of these approaches, security is a complex phenomenon.

Digital breaches are rapidly increasing despite record levels of security spending. Every organisation has to take care of digital security. Global organisations are moving to a human-centric approach that places focus on changes in user behaviour and the essential skills of a digital citizen instead of digital countermeasures.

Security and sustainability are properties of the Earth system as a whole, including the interacting physical, chemical and biological processes and global social, political and economic developments. Therefore, a business or organisation is unlikely to be sustainable if the society at large is not secure.

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

- Boddington, P. (2017). *Towards a Code of Ethics for Artificial Intelligence*. Springer. doi:10.1007/978-3-319-60648-4
- Bonnefon, J.-F., Shariffs, A., & Rahwan, I. (2015). *Autonomous vehicles need experimental ethics: Are we ready for utilitarian cars?* arXiv:1510.03346.
- Bonnefon, J.-F., Shariffs, A., & Rahwan, I. (2016). The social dilemma of autonomous vehicles. *Science*, 352(6293), 1573–1576. doi:10.1126/science.aaf2654 PMID:27339987
- Brant, T. (2016). Who should your self-driving car save in a crash? You or pedestrians? *PC Magazine*. <https://uk.pcmag.com/electronics/82490/who-should-your-self-driving-car-save-in-a-crash-you-or-pede>
- Doyal, L., & Gough, I. (1991). *A Theory of Human Need*. Macmillan. doi:10.1007/978-1-349-21500-3
- Dutton, W. H. (2017). Fostering a cyber security mindset. *Internet Policy Review*, 6(1). <https://policyreview.info/node/443/pdf>
- Eggenschwiler, J. (2017). Accountability challenges confronting cyberspace governance. *Internet Policy Review*, 6(3). <https://policyreview.info/node/712/pdf>

- Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, 7(2). <https://policyreview.info/node/788/pdf>
- Fraser, N., & Honneth, A. (2003). *Redistribution or Recognition: A Political-Philosophical Exchange*. Verso. doi:10.1002/9780470756119.ch54
- Frigo, G. (2018). *The energy ethic and strong sustainability: Outlining key principles for a moral compass*. In *Strongly Sustainable Societies: Organising Human Activities on a Hot and Full Earth*. Routledge.
- Gasper, D. (2015). *Human security: From definitions to investigating a discourse*. In *Routledge Handbook of Human Security*. Routledge.
- Honneth, A. (1995). *The Struggle for Recognition: The Grammar of Social Conflicts*. Polity.
- Honneth, A. (2007). *Disrespect: The Normative Foundations of Critical Theory*. Polity.
- Lehtonen, T. (2018). *Sustainable investment and degrowth*. In *Strongly Sustainable Societies: Organising Human Activities on a Hot and Full Earth*. Routledge.
- Martin, M., & Owen, T. (2015). *Introduction*. In *Routledge Handbook of Human Security*. Routledge.
- Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, 50(4), 370–396. doi:10.1037/h0054346
- Myerson, R. B. (1997). *Game Theory: Analysis of Conflict*. Harvard University Press.
- Neiman, S. (2015). *Evil in Modern Thought: An Alternative History of Philosophy*. Princeton University Press.
- Nemati, H. (2008). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications*. Information Science Reference. doi:10.4018/978-1-59904-937-3
- Ortmeier, P. J., & Meese, E. III. (2009). *Leadership, Ethics and Policing: Challenges for the 21st Century* (2nd ed.). Pearson.
- Pernice, I. (2019). Protecting the global digital information ecosystem: A practical initiative. *Internet Policy Review*, 8. <https://policyreview.info/articles/news/protecting-global-digital-information-ecosystem-practical-initiative/1386>
- Pew Research Center. (2019). *Public's 2019 Priorities: Economy, Health Care, Education and Security All Near Top of List*. <https://www.people-press.org/2019/01/24/publics-2019-priorities-economy-health-care-education-and-security-all-near-top-of-list/>
- Sen, A. (2015). *Birth of discourse*. In *Routledge Handbook of Human Security*. Routledge.
- Singer, P. (2016). *Ethics in the Real World: 82 Brief Essays on Things That Matter*. Princeton University Press.
- Smith, A., Voß, J.-P., & Grin, J. (2010). Innovation Studies and Sustainability Transitions: The Allure of the Multi-level Perspective and Its Challenges. *Research Policy*, 39(4), 435–448. doi:10.1016/j.respol.2010.01.023

Staub, E. (2003). Notes on cultures of violence, cultures of caring and peace, and fulfillment of basic human needs. *Political Psychology*, 24(1), 1–19. doi:10.1111/0162-895X.00314

Tainter, J. A. (2006). Social complexity and sustainability. *Ecological Complexity*, 3(2), 91–103. doi:10.1016/j.ecocom.2005.07.004

The World Commission on Environment and Development. (1987). *Our Common Future*. Oxford University Press.

Togelius, J. (2011). A procedural critique of deontological reasoning. *DiGRA '11: Proceedings of the 2011 DiGRA International Conference: Think Design Play*, 6. <http://www.digra.org/digital-library/publications/a-procedural-critique-of-deontological-reasoning/>

United Nations Commission on Human Security. (2003). *Human Security Now*. United Nations.

United Nations Development Programme. (1994). *Human Development Report*. Oxford University Press.

Wittgenstein, L. (1965). A lecture on ethics. *The Philosophical Review*, 74(1), 3–12. doi:10.2307/2183526

KEY TERMS AND DEFINITIONS

Absolute Safety: Wittgenstein’s term for the paradoxical state of mind in which one is inclined to say, “nothing can injure me whatever happens.”

Comprehensive Security: A state of preparedness for the threats and risks to vital functions of society.

Cyber Security: The practice of ensuring the integrity, confidentiality, and availability of information; a set of tools, approaches and technologies designed to protect networks, devices, programmes, and data from attacks or unauthorised access.

Digital Security: The practice of securing one’s identity, assets and technology in the online and mobile environments.

Information Security: The practice of protecting all information assets whether in hard copy or in digital form.

Safety: A tool or measure that reduces hazards; a place or position where there is no danger.

Security: The condition of being protected both from intentional and non-intentional harm and both from moral and natural evils.